UNCLASSIFIED 24 JUL 1984

ORD-0713-84

14 June 1984

MEMORANDUM FOR: Distribution

STAT FROM : [redacted]
RECON/Guard Program Manager
Information Systems Research Division
Processing and Analysis Technology Group
Office of Research and Development

SUBJECT : RECON/Guard Program: Status Report 12 June 1984

REFERENCES : 1. ORD-0564-84 dtd 4 May 1984
2. On Conversion of Prototype Guard to a Production Guard (Sytek, Inc.) dtd 22 May 1984 (Attached)

1. The Security Evaluation Phase of the RECON/Guard program has been successfully completed. The security function of the Prototype Guard System was subjected to rigorous testing by OS/ISSG, the J. P. Anderson Co., OCR, and ORD. The environment for this testing included a test database of 2K RECON records plus a system level trap door program, the Guard Test System (which is capable of emulating both the COINS-HAS and the RECON Test Database) which contains another trap door program, and non-optimal interfaces (as discussed in Reference 1). Thus rigorous testing was conducted in a very hostile environment. The creation of such a hostile test environment would not be feasible using the real RECON database and/or the real COINS-HAS. ISSG and the Anderson Co. are preparing reports on the results of their security testing.

2. User/operational testing of the Prototype Guard System was conducted and completed by the OCR project team headed by STAT [redacted] OCR/IAB. The technical expertise, diligence, and STAT conscientious participation of [redacted] and the OCR team were an integral factor in the successful conclusion of this effort. As stated in Reference 1, the results of the OCR testing will be used in the development of an operational Guard System. [redacted] is STAT preparing a report on the results of OCR operational testing.

3. With the completion of the security and user/operational evaluation of the Guard Concept and the Prototype Guard System, we are now ready to begin the final effort in the Agency's Guard

UNCLASSIFIED

SUBJECT: RECON/Guard Program: Status Report 12 June 1984

Development Program. This final effort will be the development of the operational/production Guard System. The operational Guard System will serve several applications including the actual Community RECON application. Preliminary steps in the operational Guard System development will take place during 4th Qtr. FY84, using the Prototype Guard System as a developmental testbed.

4. It should be noted that the Prototype Guard System was not structured for full operational deployment, rather to prove a security concept. This issue is discussed in detail in Reference 2. Also the RECON Test Database was structured slightly different from the real RECON database, thus providing an additional security cushion if real RECON had been inadvertently accessed.

5. Wrap-up activities for the Prototype Guard Program will include briefings on the Guard software verification procedures, results of the Prototype Evaluation, and use of the Guard Concept in various types of applications (i.e., database encryption). Also the design teams from proposed Guard applications (i.e., FBIS, CIRS) should brief the contractor on their available specifications. Thus a smooth, efficient transition into the operational/production Guard System development can be achieved.

STAT

Attachment: a/s

Distribution:
1 - D/ORD
1 - DD/ORD
1 - D/OCR
1 - D/ODP
1 - C/PATG/ORD
1 - C/ISRD/PATG
1 - RECON Committee Members
1 - Contract File (Original)
1 - ISRD Chrono, wo/att.
1 - CWK Chrono, wo/att.
1 - ORD Registry, wo/att.

STAT ISRD/ORD/DD/S&T

22 May 1984
DLC-006-84
5003-M

STAT [redacted]

Office of Research and Development
Washington, DC 20505

Ref: Contract 82f770400

STAT Dear [redacted]

Enclosed please find information concerning the conversion of the Prototype Guard System into an Enhanced Prototype Guard System for use in an operational environment.

Sincerely,

SYTEK Incorporated

Dan L. Collier
Project Manager

DLC:kw

1225 CHARLESTON ROAD, MOUNTAIN VIEW, CALIFORNIA 94039-7225 • TELEPHONE (415) 966-7300
TELEX I: TLX 176393 TELEX II: 9013795086

On Converting the Prototype Guard to a Production Guard

Introduction

A question has arisen as to the suitibility of modifying the Prototype Guard System to become a Production or Operational Guard System. The Prototype Guard System was conceived to prove a concept, and in doing so, tradeoff decisions were made that increased flexibility in design and implementation at the expense of attributes one normally associates with a true operational or production system. For example, the experimental Prototype Guard System that is currently functioning lacks the user friendliness, speed, and stability necessary in a production or operational system. None of these attributes were considered important in proving the Guard concept. Sytek strongly recommends that there be no attempt to convert the Prototype Guard System into a Production Guard System. There are many reasons for this recommendation, some of which are outlined in this paper.

Problem Issues:

1. Updating All Response Records Within Query Space

Problem: Currently all records in the real RECON data base possess null authenticators. In response to a user query, the Prototype Guard System will list these records on the audit device when encountered and in essence 'lock up' the Guard until such records are printed. The problem is that typical user queries would cause hundreds of these records to be presented to the Online Guard.

Solution: Either all possible response records meeting the user's releasability criteria are processed by the Update Guard thus greatly slowing down effective throughput, or the Customer must design a filter to eliminate records with null authenticators from being presented to the Online Guard in response to a user query.

2. Update Guard Performance

Problem: Current Update Guard Performance is unacceptable in a production environment. For example throughput for 2000 records with category expressions now in use is two hours. Average daily input of records to RECON is from 1,200 to 1,800, thus close to two hours would be spent just keeping up with daily input to the data base. Automatic recovery from tape processing errors should be seriously investigated to allow update process completion in the event of an error on the customer supplied input tape.

Solution: The Update Guard performance must be improved. This could be realized by upgrading the existing Master SBC to a 80186

based board, and other improvements to the IO Slaves and the AGB's.

3: Poor SOID and Key Distribution Procedures

Problem: The issue of SOID operation and Key distribution cannot be improved using the Prototype Guard System hardware. There exists a high probability of AGB and/or EPROM damage on a regular basis when loading the Guard System with category expressions and Secret Keys.

Solution: The SOID and existing key distribution concept cannot be changed due to prototype hardware limitations and consequently there is no solution to this problem. AGB circuit boards and EPROMS are not designed for 'field' type use. Even skilled technicians can incorrectly insert EPROMS.

4. Unacceptable RECON Interface

Problem: The existing interface is very delicate and not reliable. It was developed for prototype testing only and was made to inhibit use in an unauthorized manner. Present protocol and operating system overhead is extensive and very complex, causing the interface to fail regularly, the opposite of what is desired in an operational or production type device.

Solution: The present interface to RECON is totally unacceptable for operational and production use. Extensive rewrite of existing Data Side code will be required based upon a new interface specification. There will need to be some programming done on the Customer's systems to accommodate a cleaner interface.

5. Slow Online Guard Throughput

Problem: The Prototype Guard was built to demonstrate feasibility of a concept in a manner that could be monitored and verified. Because of this, its throughput is relatively slow (less than an overall effective 800 baud rate). Without increasing throughput, the availability of the Guard System to a user network would be greatly decreased due to time spent processing and releasing (or not releasing) response records. The typical total time required to service a complete query is approximately fifteen minutes. This would allow only four queries per hour from a network source.

Solution: For an operational or production version, this must be increased by code optimization and hardware upgrades.

6. Test RECON and Real RECON Differ

Problem: The data base used in Guard System testing is not of the same format as that of real RECON. The record document number fields differ in the two data bases. This difference was introduced to prevent the Prototype Guard from releasing records if it was inadvertently connected to real RECON prior to Guard System certification. For the prototype to be used with the real RECON data base, rewriting of software modules would be necessary in those routines concerned with record format layout. Subsystems requiring modification include the SOID, Update Guard, Online Guard, and Guard Test System.

Solution: Either the source code rewrite is performed or all existing RECON applications software and data record layouts must be changed for system compatibility.

7. Need for Renewed Code Verification

Problem: All secure code running in an operational environment requires verification of its security properties. Without reverification of modified software, there can be no assurance of its security properties. Verification is not a trivial or rapid process.

Solution: Any modifications to security critical software of the Prototype Guard System in order to make it suitable as a Production/Operational Guard System would require complete reverification. Examples of code requiring changes are those modules dealing with record formats and authenticator computation.

8. Local vs Current Development Environment

Problem: Software development necessary to convert the Prototype Guard System into a Production or Operational Guard System cannot continue to be performed in Mtn. View. This was an acceptable situation when the Prototype Guard System was in development. The existing hardware emulation capabilities in Mtn. View have been completely surpassed in finishing the Prototype Guard development. There exists only one Update Guard System, and it is staged at the Customer's site. "Real" records only exist on site and would be needed in testing and debugging. Other than the present means of development over the telephone and overnight delivery of code changes, there is no other development environment.

Solution: All software support for the Prototype Guard System

exists in Mtn. View. Development of an operational Guard from the Prototype Guard would need to be performed on the east coast at Sytek's Bethesda offices. A development environment including a microprocessor development system would need to be set up, a programmer would need to be hired, and other miscellaneous tools constructed.

9. Delays in True Operational Guard Development

Problem: Expending effort to convert the Prototype Guard System into an Enhanced Prototype Guard System will divert resources from the design, development, test, construction and implementation of a Guard System designed from the start to serve adequately in a production or operational environment.

Solution: A decision would need to be made as to whether staff and other resources should be applied to a conversion effort at the expense of the planned true Operational Guard development.

10. Changes are Out of Scope

Problem: The changes required to obtain the reliability and throughput speed required for an operational or production Guard System from the Prototype one are beyond the scope of the existing Support Contract. This would require a new contract and funding from the Customer.

Reason: The existing support contract is to cover continued hardware and software support and maintenance of the Prototype Guard System. Evolving the Prototype Guard System into an operational/production Guard is beyond the scope of the current contract.

Conclusion

Sytek recommends that no further effort be spent in the conversion of the existing Prototype Guard System into a production or operational system. Any resulting device would only serve to frustrate Customer computer operators and network users. A guard system that addresses all of the above problems (the true Production Guard) can be developed so long as necessary resources are not diverted in a conversion effort.